TACOMS Post 2000 – Interoperability in Communications

Krzysztof Lysek, PhD
Military Communication Institute
05-130 Zegrze, Poland

k.lysek@wil.waw.pl

TACOMS POST 2000 PROJECT

In NATO, interoperable communications standardization activities have taken many forms and have used many different approaches in order to achieve this goal. In 1986, the NATO project group six (PG/6) was responsible for developing interoperable communications standards in the land combat zone. In the PG/6 report, it established the methodology to develop the interoperable communications standards, and conceived the TACOMS project.

The TACOMS Post 2000 project was sponsored through an MOU signed by a thirteen NATO nations that formed the project steering group (PSG). It was the TACOMS PSG who in turn asked the MOU nations to financially support and to provide the personnel resources to establish an international project office (IPO) that was located outside of Paris, France. France was the host organization (HO) for the project. A project manager, a principal engineer, and five systems engineers leaded the TP2K IPO from different nations who oversee the work of TAC ONE, a defence industry consortium of five principal contractors, and 13 subcontractors from each of the participating TACOMS nations. The TACOMS contract was a fixed price of 22M Euros, with a required equal work share for each of the subcontractors.

The goal for TP2K was to develop draft standardization agreements, STANAGs that will provide NATO and its coalition forces commanders with an interoperable tactical communications infrastructure. As a result of TACOMS Post 2000 project, set of 11 STANAGS was delivered to SC/6 in June 5005.

The TP2K standards will allow multinational network systems to inter-operate with the maximum of coalition operational efficiency, while the national system user and network elements maintain their value. In the STANAG 4206, and many legacy based systems interoperability is achieved by defining a common NATO standard information structures and formats, and then exchanging data over dedicated gateways that are used as portals between the systems.

TACOMS NETWORK ARCHITECTURE

The TACOMS network architecture is based on providing a shared coalition information domain with a set of common standardised user services that allow users and elements to freely roam and reconfigure, just, while the national elements can be implemented using their own choice of network technology. In this approach standardization is focused on functionality of the interoperability points, and on the performance of the intermediate elements, to make up an integrated system.

The interoperability points are defined without mandating specific networking technologies in the elements. The elements of the Wide Area Subsystem (WAS) are assumed to be complete network sections (or subnets), rather than individual switches and transmission links.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
NOV 2009	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
TACOMS Post 2000 Interoperability in Communications	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Military Communication Institute 05-130 Zegrze, Poland**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
See also ADB381488. RTO-EN-IST-088, Interoperability Issues (Questions d'interoperabilite).

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**12**	

The TACOMS network is based on the concept of "Interoperability Points" (IOP). This means, that transmission technology and protocols used inside national networks are not a concern of TACOMS standardization. The whole protocol stack is defined only for the points in which networks built by different nations are connected together at the IOP.

It is a national responsibility in implementing the TACOMS standards, to develop inter-working edge devices, which will convert data from a nationally defined form to the form defined for Interoperability Point, and to deliver the necessary user services as necessary to fulfil the network elements performance requirements.

The basic transmission rate selected for the IOP is 1Gbit/s over Ethernet. This big over-provisioning ensures that the QoS inside the IOP and limitations of resources may be located only in national networks.

The TACOMS Interoperability Points (IOPs) between network elements are not tactical gateways. Instead, they are interfaces or edge devices with additional functionality that allow for coalition-wide routing, mobility, network management, security etc. This has been developed in order to provide an agreed set of common mandatory and optional end-to-end network services like routing or battlefield directory, providing user the capability of being virtually connected to a network centric integrated tactical theatre network.

Several different User Terminal Access Points (UTAP), are specified. These UTAPs enable for terminal mobility when it is necessary to move terminal form one national network to another (for instance because of built-in unique functions).

In addition there are interfaces to non-TACOMS entities such as External Network Access Point (ENAP) and systems, allowing for connection with civilian and military ISDN and analogue networks, legacy tactical networks, IP and X.25 networks.

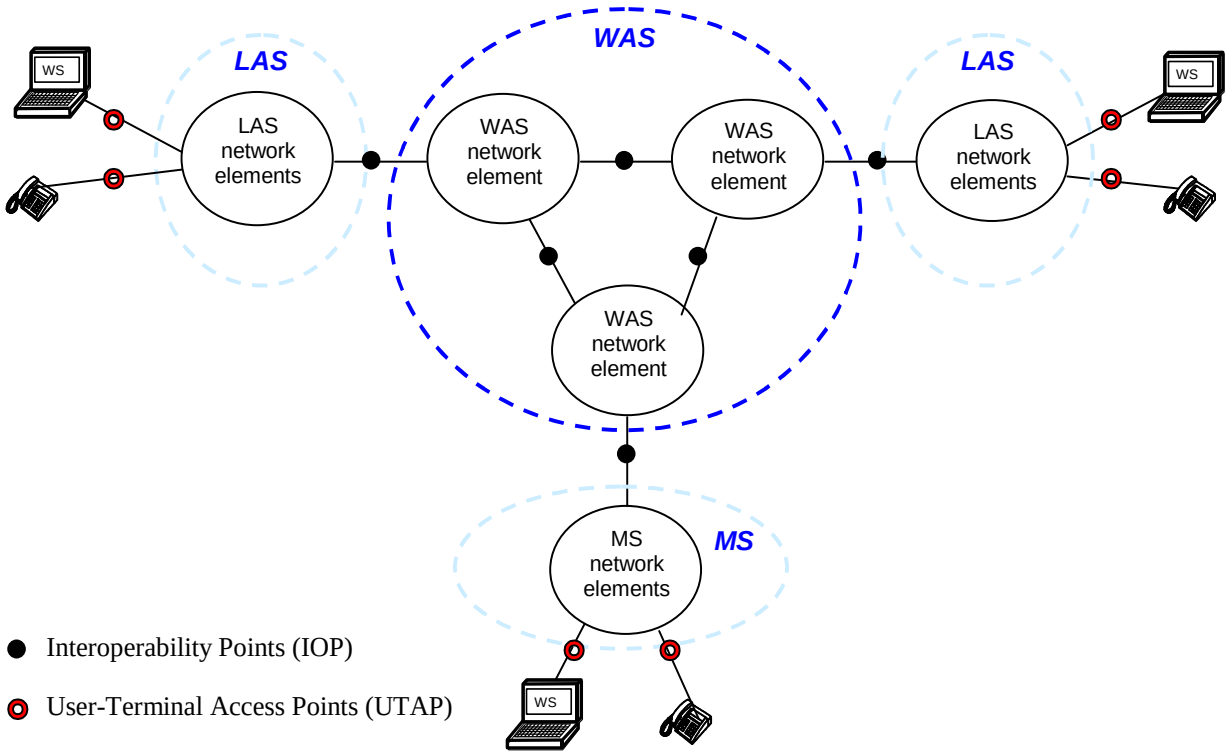

Figure 2.1: TACOMS Network Elements and Interoperability Points

From the perspective of a top-level architecture, a TACOMS networks consist of three different subsystems:

Local Area Subsystem (LAS), typically supporting Head Quarters (HQ's) and Command Posts (CPs), ranging from the main multinational HQ Land Component Command (LCC) of a Combined Joint Task Force (CJTF) or High Readiness Force HRF-HQ to a national Battle Group (BG) or Battalion Command Posts (CP) in the scenario.

Mobile Subsystem (MS), typically representing the many different types of national radio networks used to connect mobile users via national Radio Access Points (RAP) in the scenario

Wide Area Subsystem (WAS) interconnecting the many dispersed LAS and MS entities in an operational theatre as well as providing the connection to external networks such as public, private and military strategic and legacy (non-TACOMS) tactical networks.

In addition there is a System Management and Control Subsystem (SMCS) to perform the TACOMS wide network control.

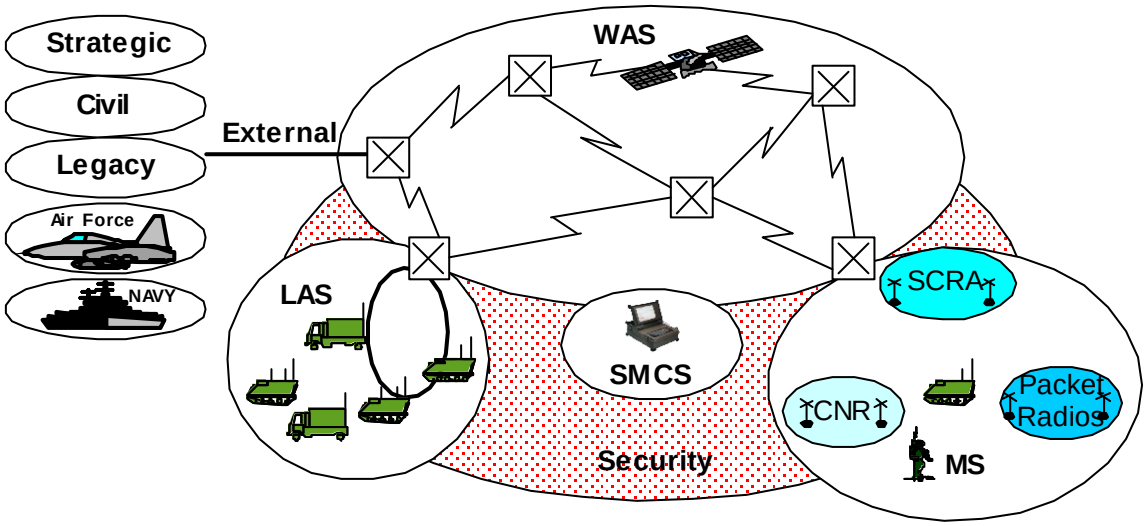

Figure 2.2: Simplified TACOMS network diagram

Each network element contains several nodes and links. Each WAS Network Element is considered as a "black-box" defined by its input/ output ports and its performance (capacity and quality). Figure 2 shows a simplified TACOMS network diagram with LAS, MS and WAS subnets and user terminals, which would be provided by different nations. Network-wide Information Security (INFOSEC) solutions provide the required security protection of the information and the components in the system.

The network elements may be implemented using different core technology, e.g.

One LAS may be based on Ethernet LAN technology or ATM with LAN emulation, and may include an ISDN PABX for voice services or implement Voice over IP (VoIP) as part of its Ethernet LAN structure;

One of the WAS network element may be using ATM in the core, while another civilian or tactical ISDN TDM technology and a third may be IP V 4 or IPV6 based;

An MS radio network may utilise a large variety and combinations of communications technologies such as CNR (Combat Net Radio), Packet Radio, Broad Band Packet Radio and SCRA (Single Channel Radio Access).

TACOMS STANDARDISATION METHODOLOGY AND CONTEXT

The TACOMS standardisation effort has taken into account major changes in the coalition land battlefield operational and technical area.

Military operations in the 360-degree battlespace will involve some form of military/political coalition within a UN/NATO/EU framework. This means that the party, or parties, that the international coalition is facing sees a multinational coalition prepared to impose its political and military strength on its territory or its assets in effective ways to maintain the interests of the World Community. It is essential that this coalition force is equipped with capabilities that are superior to any capability that such an opponent can possibly deploy. The coalition must possess immediate superiority through the kind of operational capabilities that incorporate Network Enabled Capabilities (NEC).

The TACOMS standards are NEC enablers, and the operational user requirements have been confirmed from the basis of the NATO approved MC337 (Reference 1), enhanced through an updated user services

concept described later in this document, to provide support to a tactical operational architecture as described in the NC3A study CR 149, (Reference 2).

This scenario has then been used to develop a populated operational traffic requirement database containing the anticipated Information Exchange Requirements (IER) for the planned operation of the NRF in a complex Peace Support Operation (PSO). The second development that has been taken into account to define the TACOMS standards is the technical and operational development that has led to the transformation of military planning and operation over the last few years.

Traditionally network design and its implementation involved defining the interfaces and the elements in such a way that they map onto specific equipment in the national systems.

In TACOMS, the network design is not part of the standard; direct mapping between an element and a physical device is not specified. The internal architecture (including topology, protocols, equipment scaling, etc.) of national elements is a national concern. These elements will be treated as black boxes with specified interfaces, network functions and minimum performance. Network functions include routing procedures, directory procedures, call handling functions, security services, etc.

The TACOMS standardisation methodology consisted of:

Definition of user services.

Definition of network elements:

Wide Area Subsystem (WAS) elements

Local Area Subsystem (LAS) elements

Mobile Subsystem (MS) elements

Definition of interfaces:

User Terminal Access Points (UTAP)

Interoperability Points (IOP)

External Network Access Points (ENAP)

Specification of protocols for the interfaces listed above:

Reusing as much as possible the civilian standards able to meet the requirements

Reusing military standards when there are no adequate civilian standards

Specifying enhancements to existing protocols when neither civilian nor military standards are able to meet the requirements

Specification of the protocol stack applicable to the given interface by selecting a set of protocols and tailoring them as required.

Specification of network element behaviour and network services.

Specification of network element performance.

COMMON INFORMATION ARCHITECTURE

TACOMS standards are defined to provide common information architecture to interconnect the voice, multimedia and data applications, constituting a responsive information grid for the network enabled warrior. However, from an overall system level viewpoint the standardisation of user applications are not directly included in the scope of the TACOMS standards In general TACOMS provides the transport of the traffic generated by user applications, assuring the adequate QoS, but some applications, like voice and video, are also standardised for interoperability reasons.

TACOMS standards will accommodate voice traffic with the following representations:

Pulse Code Modulation (PCM) as used in public and strategic/ tactical ISDN based networks,

Continuous Variable Slope Data (CVSD) modulation (STANAG 4209) standard voice coding schemes, as used in current tactical radios and trunk networks,

Standard MELPe (STANAG 4591) is expected to become the main representation of voice in TACOMS.

The TACOMS standards themselves will not define or introduce any further voice encoding schemes. Other voice encoders such as G.723 or G.729D that come as parts of the civilian signalling protocols will not be excluded though.

TACOMS is a set of network standards with a service-oriented architecture all other user applications such as video and multimedia, collaborative planning systems, shared intelligence support systems are outside the scope of TACOMS as detailed areas for standardisation. Nonetheless, these and other future applications will be able to use a TACOMS network transport services through its Service Level Specifications (described in following section).

TACOMS encompasses all required interconnect standards allowing users, equipment and vehicles to be interconnected with cables and connectors where the nations units are collocated or requiring only short cable connections for their interconnection.

Secure communication in TACOMS is based on end-user-to-end-user system security solutions for voice and data. Detailed encryption standards, however, are currently being defined inside the “Future Narrow Band Digital Terminal” (FNBDT) or its NATO equivalent “Secure Communication Interoperability Protocol” (SCIP) and military enhanced IPsec. Therefore TACOMS standards contain references to these future standards.

TACOMS STANAG STRUCTURE

The Head STANAG is made to provide the informative overview of the standards, and to describe their operational and technical context.

Annexes to the Head STANAG contains informative material such as system requirements, user services etc., and some normative elements related to guidance to implementers for completing the Conformance Statements (NPICS, NSPICS, NPRL) and to the (common) standard Lexicon used throughout the eleven TACOMS STANAGs.

Ten further STANAGs with a varying number of Annexes are then provided to give the entire set of required standards to ensure total overall compliance with the TACOMS operational principle.

These STANAGs are organised such that a nation that ratifies the entire structure may choose to implement the subset they need in order to fulfil their specific role in the coalition force structure they will participate in.

The following contains the list of the STANAGs in abbreviated form for illustrative purposes:

STANAG 4637: TACOMS Head STANAG

STANAG 4638: TACOMS Elements Performance

STANAG 4639: TACOMS Interfaces

STANAG 4640: TACOMS Low Layers Specifications

STANAG 4641: TACOMS ISDN Access Protocols

STANAG 4642: TACOMS IP Access Protocols

STANAG 4643: TACOMS Connection Oriented Network Protocols

STANAG 4644: TACOMS Connection Less Network Protocols

STANAG 4645: TACOMS Radio Protocols

STANAG 4646: TACOMS Management Protocols

STANAG 4647: TACOMS Gateway Protocols

QUALITY OF SERVICE CONCEPT IN TACOMS - SLS AND SLA

In order to seamlessly interoperate the various national systems, there has to be a common understanding of the services that need to be supported by all networks. The TACOMS architecture is therefore service oriented and the standards will include Service Level Specifications (SLS) and will invoke Service Level Agreements (SLA).

For TACOMS, most IOPs between network elements carry an aggregate traffic flow consisting of two “logical channels” belonging to two "traffic handling classes".

“Connection Oriented” (CO): this “logical channel” will carry traffic that requires a specific QoS guarantees, i.e. typical real-time, circuit mode services like voice and continuous streams of data.

“Connection-Less” (CL): handling of traffic with different QoS guarantees, i.e. traffic of a nature where the end application can cope with a less continuously streaming flow of information

These two “logical channels” are standardised with different signalling, “call handling” mechanisms and routing and in general have no inter-working. In the TACOMS IOP, both logical channels are transported in one physical, “service integrated” interface based on civilian Ethernet standards.

According to TACOMS standards, traffic coming from applications uses services divided into five groups, defined in Service Level Specifications. Definition for each SLS contains QoS requirements, expressed in packet loss ratio, packet delay, packet delay variation, and call blocking probability.

The number of applications is not defined nor limited. Assignment of a particular application to given SLS is not standardized as well. Only limited number of features and requirements for limited number of services was standardized, for example voice coding schemes (MELPe, CVSD, PCM), transmission rates

(2.4kbit/s, 16kbit/s, 64kbit/s) and voice transcoding process.

This approach was chosen because it is not possible to predict which applications will be used in future network and which will be more or less important. Moreover, the final assignment may be more or less efficient depending on technology and topology of the network and different for different deployments.

Because of different QoS requirements it is not possible to transfer data between applications assigned to different SLSes. It means, that the assignment must be unified in the whole network.

These contrary requirements of flexibility and unification in assignment of applications to SLSes caused, that Service Level Agreement (SLA) concept was introduced in TACOMS. Every time in preparation phase before the establishing of the TACOMS network all of the services will be assigned to the appropriate SLSes in the unified manner. It may be preceded by a kind of negotiation process in which technological, topological and traffic constrains will be taken into account. To simplify this process an example of SLA is a part of TACOMS standards, not as a requirement, but as a recommendation.

TACOMS AND NNEC

To provide guidance to nations and NATO for CIS related matters, the NC3A developed a study [4] and has produced a draft report that contains recommendations to help nations in achieving a coalition NNEC in the medium to long term. This document describes the required capability for the 4 components of a NNEC infrastructure (Information systems, communication services, information assurance and operation and management) for NNEC 2012. A separate chapter is dedicated to the processes and policies that need to be changed, developed or improved to support the full life cycle operation and maintenance of a NNEC infrastructure.

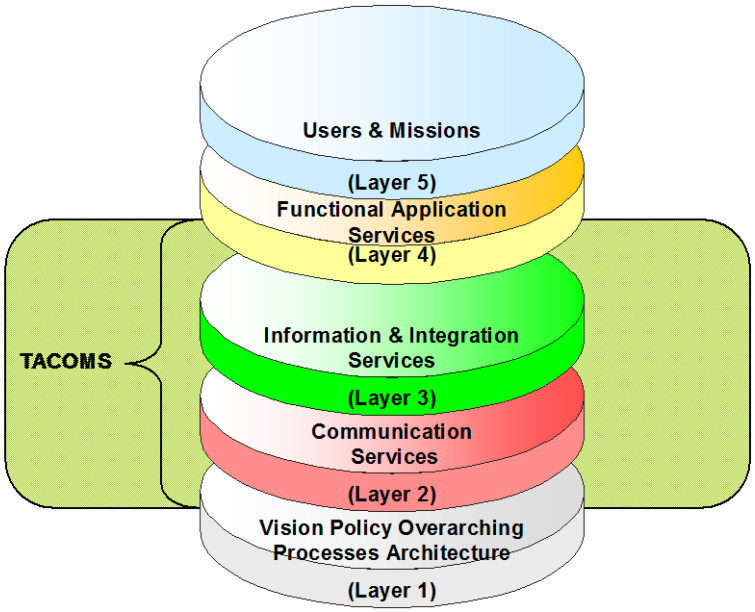

Figure 7.1 NNEC Infrastructure Requirements

The figure above illustrates how the NEC concept covers many areas in different layers. It should be highlighted, that the major part of them, and probably the most important, are related to human and organizational factors, with adopting new way of thinking – network-centric thinking. This transformation

to network centric operations is fundamental and must be taken into account when the nations vision and NEC goals are defined, in training of its personnel and in its acquisition planning processes.

This transformation to network–centric operations must be achieved through use of advanced communication networks, because "It all begins with infrastructure". [1]

TACOMS interoperability standards developed on this basis meet the NNEC communication services, information and integration services and information assurance tenets as described in the following sections.

COMMUNICATION SERVICE TENETS

- *Evolve to a packet-switched infrastructure* – According to TACOMS Post 2000 assumptions, technology inside national network elements is not defined but national concern. The protocol stack is defined precisely for Interoperability Points and in this case solution based on Ethernet (packet based technology) was selected.
- *Build the environment in a layered, modular manner to simplify upgrading to newer versions of standards*. – This layer-based approach was always used in TACOMS standardisation.
- *Move toward convergence of voice, video, and data traffic on a "single network"* – TACOMS Interoperability Point is a good example of such convergence – every kind of traffic is transported through a single link.
- *Implement IPv6 for standard communications in NATO* – In fact IPv6 was selected as a technology used in Interoperability Point, because it is easier to achieve interoperability with existing solutions.
- *Provide network connectivity to all end-points such as wide- and local area networks and direct connections to mobile end users* – That is exactly in line with the TACOMS standards, including user, terminal and network mobility.
- *Support differentiated management of Quality-of-Service (QoS) to ensure required levels of availability by application and function* – TACOMS QoS structure, based on Service Level Specification and Service Level Agreements is a powerful tool to ensure QoS for both, connection-oriented and connectionless traffic.

INFORMATION AND INTEGRATION SERVICES TENETS

- *Adopt a service-oriented architecture* – Service-oriented architecture is a base of TACOMS
- *Build an open architecture* – TACOMS protocol stack is defined using layered model; TACOMS-based network is ready for support existing and future services.
- *Design to assure scalability of services and their availability to all users* – Applications were not a subject of TACOMS standardisation, but to ensure basic interoperability voice coding, transcoding and negotiation protocols and data rate adaptation schemes are defined. This gives access to basic

network services even for users of legacy, TACOMS non-compliant networks. Traffic generated by other services may be transported using one of defined SLSes with guaranteed QoS, to any user.

- *Accommodate heterogeneity of user platforms and servers, from high-end to disadvantaged* – This tenet is related with implemented applications more than network equipment, but TACOMS puts no restriction in this area.
- *Support Enterprise Service Management in a decentralized manner* – TACOMS gives full autonomy national network elements under condition that basic requirements, described in Service Level Agreement in planning phase, are fulfilled.
- *Make data visible, accessible, understandable, interoperable, and trustable* – This is a task for application more than for the network, but when necessary (voice transcoding) TACOMS standards define this.

INFORMATION ASSURANCE TENETS

- *Support end-to-end encryption to protect authorized users access to information* – End-to-end encryption based on SCIP and IPsec are basis of TACOMS INFOSEC Functional View.
- *Mediate security assertions to facilitate passing security related information between systems, processes, and domains* – this was taken into account in INFOSEC Functional View, but the full and consistent security policy must be defined by approved body.
- *Manage identity and privileges effectively* – TACOMS defines user affiliation and authentication protocols, which together with TACOMS Battlefield Directory allow for managing privileges and support user mobility.
- *Support effective, secure cross-security-domain information exchange* - this was taken into account in INFOSEC Functional View, but the full and consistent security policy must be defined by approved body.

CONCLUSION

TACOMS is an interoperable tactical communications methodology. To effectively use the combat power generated from the linking of systems of networks and finally in the operation of the warfighting enterprise it is necessary to have a suitable network infrastructure, i.e. a set of technological capabilities able to support a range of missions. In multi-national operations, high-level communications interoperability must be ensured. It is not enough to only have national networks connected thru gateways, it is necessary to have unified, and interoperable service oriented networks. In a coalition environment the infrastructure will be composed of different, often, different networks. The challenge in this environment is to still be able to provide homogeneous services across these heterogeneous networks. Therefore the services provided by the individual infrastructure components (com service architecture, info & integration services architecture, information assurance and CIS management) as well the infosphere definition should be harmonized between coalition members. TACOMS standards achieve this capability and thus will serve as a key enabler of NNEC and NCO/W in the tactical land environment of the 360-degree battlespace.

TACOMS is a methodology delivered in the form of paper STANAGs. These standards must be implemented by nations to enable NATO and coalition forces network centric operations

REFERENCES

[1] NATO Military Operational Requirements and Communication Architecture for Interoperable Tactical Communication Systems for the Land Combat Zone Post 2000 Tactical, MC 337

[2] TACOMS Web site, http://www.tacomspost2000.org

[3] Tactical Interoperable Communications Standards (TACOMS) A Key Enabler to achieving NATO Network Enabled Capabilities, C. Echols, K. Lysek, IST-054/RSY-015, Rome, 18-19 April 2005

[4] D. S. Alberts, J. J. Garstka, F. P. Stein, Network Centric Warfare, 2002

[5] R. Van Engelshoven, R. Porta, J. Busch, ea. NNEC Study - CIS Related Issues, draft v.4.2 NC3A, 2004

[6] J. Grainger, E. Ross, G. Dodgeson Tacoms Operational C2 and Information Architectures, NC3A, Jul. 2003